Physician Comments on Privacy and Security for Central Illinois Health Exchange

Key Considerations

The following are key privacy and security considerations.

1. ***Comply with current standards for patient confidentiality***. Clinicians have always recognized the importance of patient confidentiality. With HIPPA, this tradition is enforced with major penalties. Additional regulations above and beyond HIPPA place a major burden on healthcare providers. Many patients receive care in more than one state and many healthcare providers practice in more than one state. Different state laws creates confusion and additional burdens for patients, healthcare providers and healthcare organizations.
2. ***Support quality patient care***. The best patient care requires a complete patient record. If key information is missing such as a medication or a problem that affects disease outcome such as depression some patients will suffer complications and death. A patient without medical training is not able to judge what is important. Most patients do not know that gonorrhea could be a cause of ankle pain which leads to their podiatrist appointment.
3. ***Laws that are easy to follow***. Adding extra steps to healthcare visits burdens patients clinicians and healthcare organizations. Software vendors have limited dollars to spend to comply with new unique state regulations. A patchwork of laws for different diseases makes compliance even harder.
4. ***Fair for patients and clinicians***: What is private and how it is maintained should be easy to understand and clear to patients and clinicians. Ideally privacy should be a collaboration between patients and their caregivers. We believe most patients trust their doctor more than insurance companies and government. A patient cannot opt out of mandated disease reporting. Physicians are very concerned when key information needed for care such as a prescribed medication list or the diagnoses for past visits are available to insurance companies and not the treating physician.

Patient Choice

1. Most physicians believe that patients should not be able to opt out of information needed for coordinated care. For sensitive information such as visits to a psychiatrist or a psychologist and care at drug treatment centers there is a long history of not making visits generally available. Most clinicians would agree with this extra protection.

Permitted Uses for Patient Data

1. Physicians believe strongly that a complete medical record is needed to provide the best possible care of the patient current HIPPA regulations should be used as a national standard.

Aggregated Data

1. Institutional Review Boards (IRB) already exist to protect patients. There is an established legal structure for them and they commonly review research project

involving patient data. We believe this well establhised patient protection system should be used for IRBs should be used for HIE data.
2. If data is de-identified and there is IRB approval, we believe it should be available for quality improvement and research.
3. If data is not de-identified and needed for quality improvement or research we believe that it should only be available after IRB review that the benefits outweigh the risks. IRB's currently perform this function.
4. Most clinicians would prefer to restrict commercial use of the HIE data

Granularity of Patient Data

1. Most current software programs will not support granular privacy flags. Even if all HIE software could do this in the future, there are a huge number of legacy software systems that must send and receive data to the HIE that do not have this capability.

Sensitivity of Patient Data: Safeguards for Certain Personal Health Information

1. Most clinicians do support extra protection for records of sensitive such as visits to psychiatrist and psychologist as well as records for drug treatment centers.
2. Clinicians do not support efforts to stop inadvertent disclosure by eliminating depression from problem lists or by not displaying antidepressant on medication lists. Not only is this not possible using current technology it can lead to patients dying because of drug it interactions and other negative events due to missing information.
3. Clinicians who are not mental health professionals also do not support creating a separate visit note for the mental health portion of a wholistic primary care visit. Ultimately, every primary care visit has a mental health component that cannot be easily separated from the rest of the care.

Fostering Public Trust in HIE's: Enforcement and Mitigation Strategies

1. Clinicians do ongoing auditing of HIE use to ideally identify problems in real time.
2. Clinicians also support allowing patients to see their entire record and obtain an audit of all people who have viewed their record.
3. Penalties for misuse need to be real.

A Potential Framework for Patient/Clinician Collaboration

Propose the following which could provide a clear framework for both patients and providers.

A visit to a location should have three standard levels of privacy. The location would use privacy forms and other communication to make the level of privacy clear. The level could always be the same for some locations such as a psychiatry office or vary by visit in other locations such as a multi-specialty office with a psychologist.

1. All information from the visit would be available for coordination of care with other providers.
2. Information on a standard healthcare summary such as a CCD including medications, problems, visit diagnoses, immunizations and procedures would be available for coordination of care but not the visit note.

3. No information from the visit will be shared with the HIE and information would only be available with the patient's consent. (If this is used, patients should be advised of the risks of hiding their information.)

This transparent, informed standard would provide clear guidance for patients and providers on what could be shared.

Thank you for your consideration of the above comments.

Sincerely,
David E Trachtenbarg
David E Trachtenbarg, M.D.